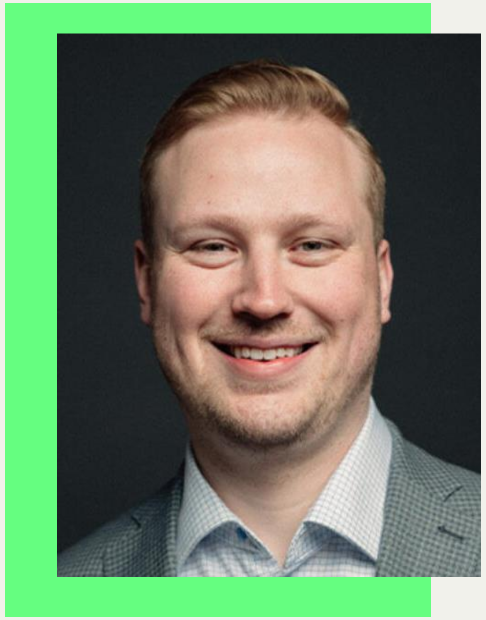
HIPAA and AI: Challenges and Solutions for MedTech

Paul Rothermel, J.D., CIPM

May 8, 2025

GARDNER
FDA LAW FIRM

Presenter Introductions



Paul Rothermel
Attorney
prothermel@gardner.law
Phone: 651-364-7514
GARDNER
FDA LAW FIRM

Paul Rothermel specializes in privacy, cybersecurity, technology and AI matters, including HIPAA, GDPR, and other state, federal, and international privacy laws as well as health care compliance matters. Before practicing at Gardner Law, Paul worked for a large medical device manufacturer advising on innovative health care technologies, clinical research, and vendor risk management. Previously, Paul counseled health and human services programs on privacy and cybersecurity compliance including HIPAA implementation. Paul is a licensed attorney in Minnesota and is credentialed as a certified information privacy manager through the International Association of Privacy Professionals.

Introduction

- Agenda
  - Overview of HIPAA, AI, and related laws
  - Key considerations for med tech applications
  - Questions?

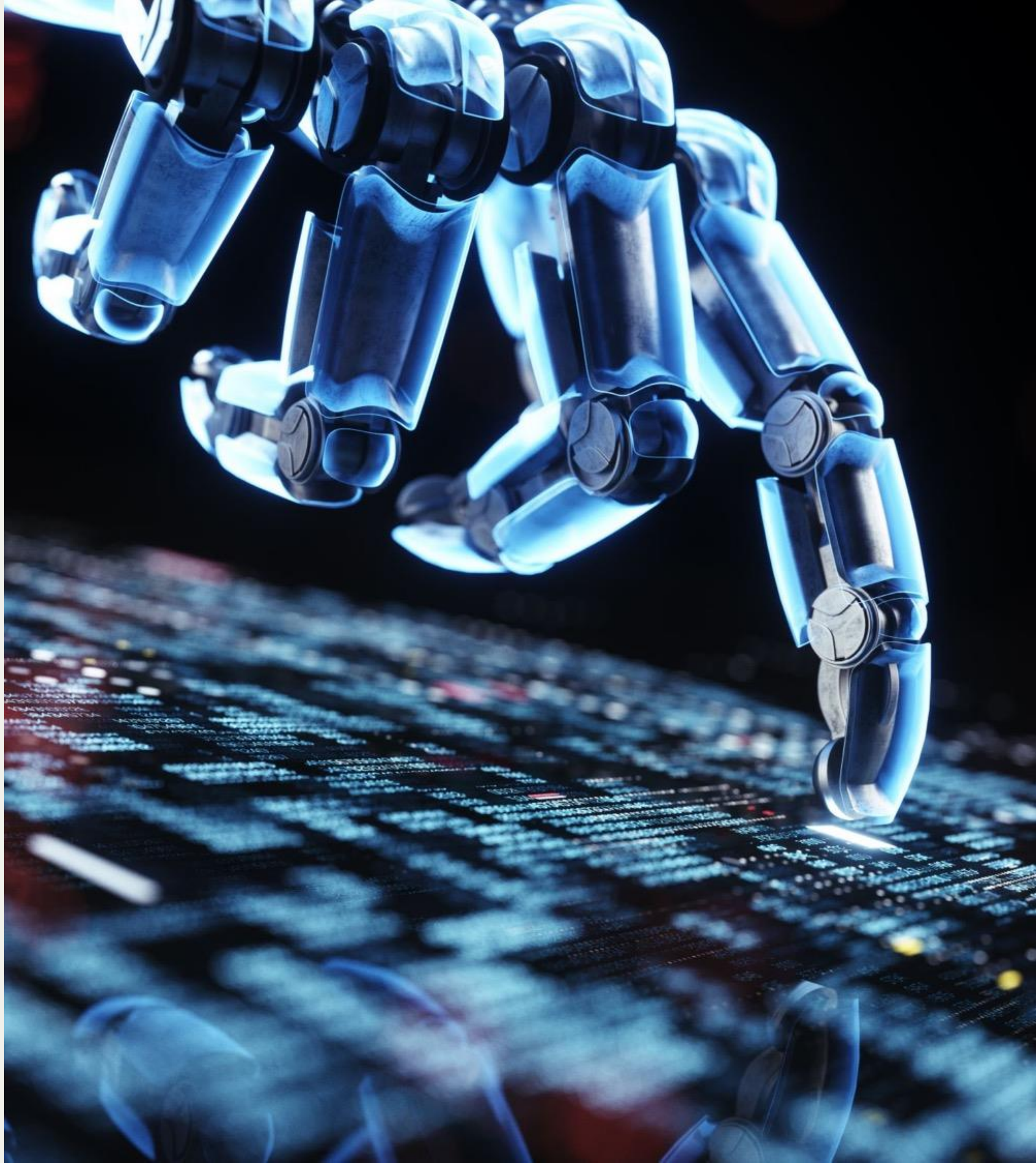
- Objective:
  - Understand how HIPAA, state privacy laws, AI use and development, and AI regulation interact
  - Learn how to more safely navigate privacy risk and AI in the med tech industry

AI in Healthcare

GARDNER
FDA LAW FIRM

Artificial Intelligence / Machine Learning

- Artificial Intelligence (AI) has been broadly defined as the science and engineering of making intelligent machines, notably intelligent computer programs.
    - AI can use techniques such as models based on statistical analysis of data, expert systems that primarily rely on if-then statements, and machine learning.
- Machine Learning (ML) is an AI technique that can be used to design and train software algorithms to learn from and act upon data.
    - Software developers can use ML to create an algorithm that is ‘locked’ so that its function does not change, or ‘adaptive’ so its behavior can change over time based on new data.



Why is AI/ML important in healthcare?

AI and ML are used to derive new insights from the enormous amount of data generated during the delivery of healthcare

AI/ML can learn from real-world use and experience and can improve its own performance

Manufacturers are using AI/ML to innovate their products to assist healthcare providers and improve patient care

Efficiency or improved accuracy from delegating tasks to AI/ML (e.g., agentic AI or automated decision-making)

AI/ML in Healthcare

- Applications:
  - Help make sense of immense volumes of health care data
  - Pre-op planning/predicting post-surgical outcomes
  - AI-assisted surgery or treatment planning
  - Diagnostics
  - Generative AI (used by marketers, developers, doctors, etc.)
  - Agentic AI (decision-making AI intended to increase efficiency)
  - And more...

HIPAA/State Privacy Law Overview

GARDNER

FDA LAW FIRM

HIPAA and HITECH

- Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), 42 U.S.C. 1320d, as amended, and implementing regulations at 45 C.F.R. §§ 160-164

- Health Information Technology for Economic and Clinical Health Act’’ (“HITECH”) 42 U.S.C. § 17935

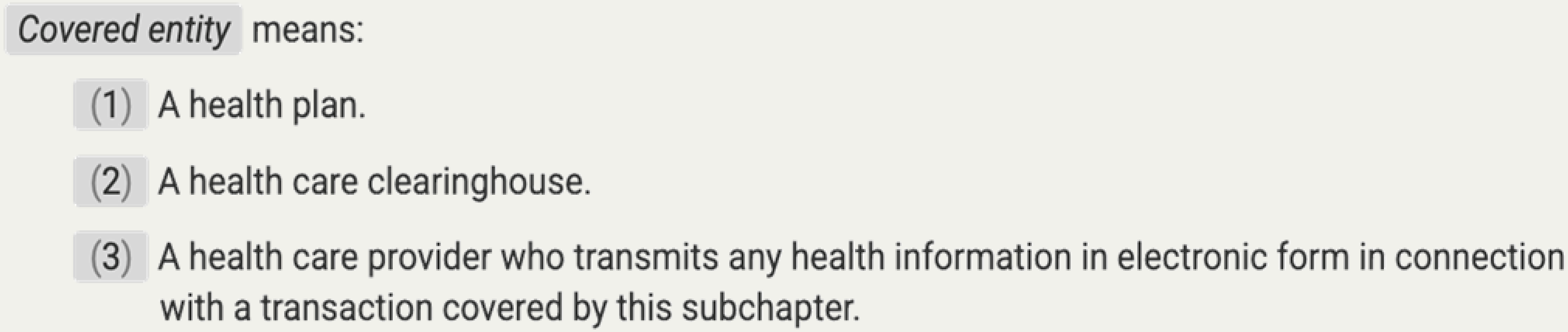
GARDNER
FDA LAW FIRM

HIPAA and HITECH

- Sets privacy and security standards for “covered entities” and “business associates”, including:
  - DME manufacturers, laboratories;
  - Many connected device makers;
  - Other service functions (e.g., reimbursement support)
- Governs use and disclosure of Protected Health Information (“PHI”)
- Restricts external sharing/internal use of PHI
- Security safeguards

Covered entity

45 C.F.R 160.103:



Covered entity means:

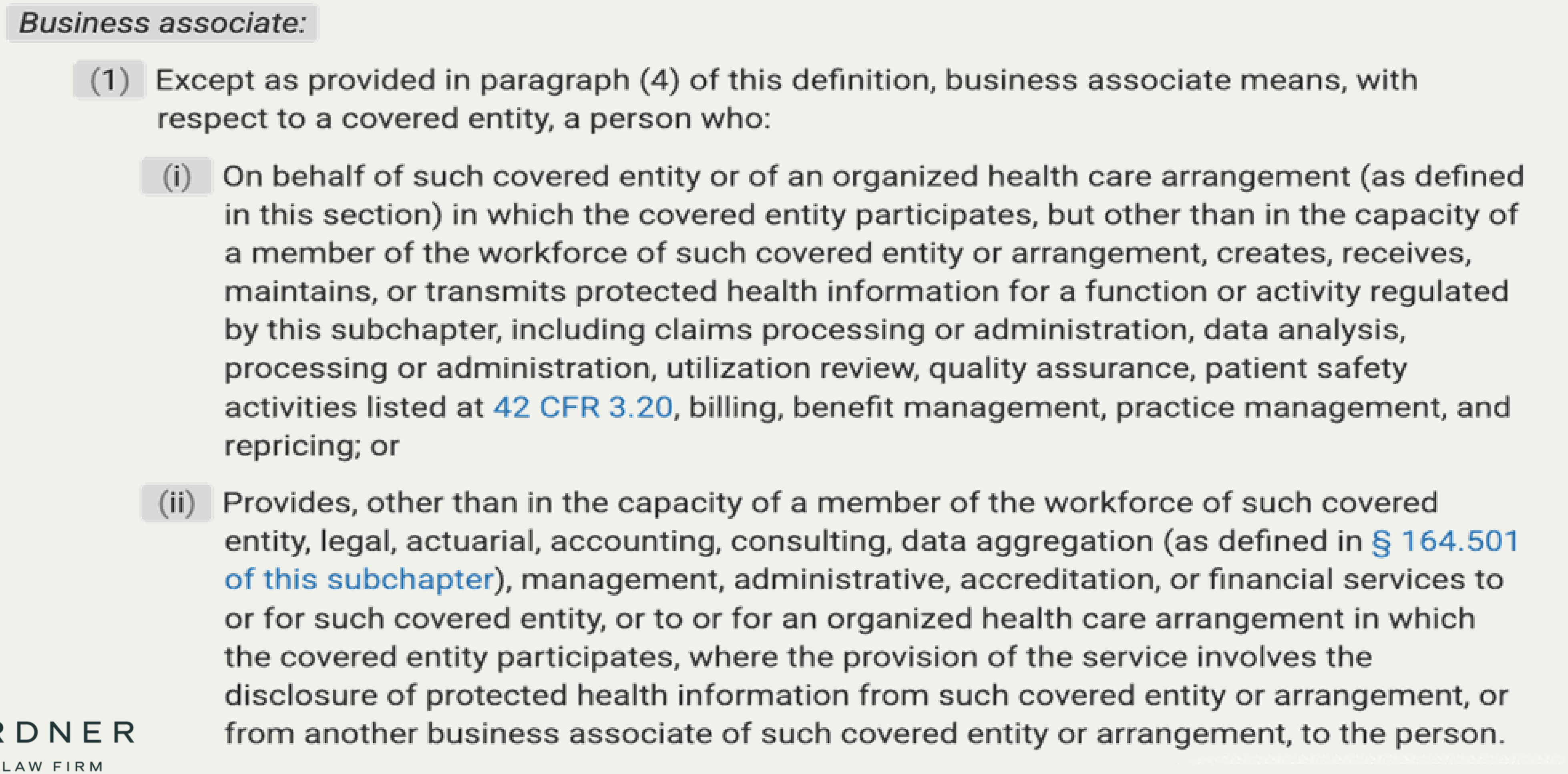
(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Business associate

45 C.F.R 160.103:



Business associate:

(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

Business associate or not?

- Exceptions to business associate designation include disclosures for:
  - Treatment, payment, health care operations (45 C.F.R. 164.506(c))
  - Patient authorization (45 C.F.R. 164.508)
  - Public health, including to FDA-regulated companies (e.g., patient registration or adverse event reporting) (45 C.F.R. 164.512(c))
- Common business associate activities in drug and device manufacturing:
  - Connected products or services that process PHI in the cloud on behalf of the customer
  - Reimbursement/product support programs, prior authorization support, or other related activity
- Business associate definition
- (45 C.F.R. § 160.103)
- See also HHS FAQ #490

Deidentified PHI

- HIPAA does not regulate health information that is deidentified:
  - Removal of 18 identifiers or expert determination per 45 C.F.R. 164.514.
  - Covered entity cannot have "actual knowledge" information could be reidentified
- Many key state privacy laws exempt deidentified PHI, e.g.,:
  - The California Consumer Privacy Act (1798.146(a)(4)) does not apply to information deidentified in accordance with HIPAA and derived from PHI subject to HIPAA or the California Confidentiality of Medical Information Act
- Properly deidentified PHI can be used for AI applications more freely
- Note: Business associates may not deidentify PHI without covered entity's authorization

Research and PHI

- PHI may be used and disclosed for research purposes with:
  - Patient authorization (45 C.F.R. 164.508);
  - IRB or privacy board waiver (45 C.F.R. 164.512); or
  - In certain contexts, for reviews preparatory to research if certain safeguards are employed.
- PHI collected for research and used to train AI will generally need to rely on patient authorization or, where appropriate, on a waiver.
- Covered entities may also deidentify PHI for research use or use to create a "limited data set".
  - Limited data sets are partly deidentified PHI which may be used and disclosed with a data use agreement for limited research and health care operations purposes (see 45 C.F.R. 164.514(e)).

Health care operations

- PHI may be used and disclosed for the health care operations of the covered entity (45 C.F.R. 164.506).
- “Health care operations” is a broad designation, covering activities like quality improvement, training, auditing, care coordination, non-research outcomes evaluation, case management, and other internal functions supporting the operations of the covered entity (see 45 C.F.R. 164.501)
- With appropriate safeguards, AI tools could be deployed to process PHI in support of the health care operations of the covered entity.

What is protected health information (PHI)?

- HIPAA (45 C.F.R. 160.103)
- *PHI* is identifiable information (including demographic information) that:

  (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

  (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

    (i) That identifies the individual; or

    (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

- Excludes:
  - Information in employment records,
  - Educational records protected by the Family Educational Rights and Privacy Act (FERPA); and
  - Information about persons deceased more than 50 years.

GARDNER
FDA LAW FIRM

Personal information (California)

- California Consumer Privacy Act (Title 1.81.5. California Consumer Privacy Act of 2018 1798.140(v)(1))
- ***Personal information*** **means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household**. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household [...]
- Examples from the statute:
  - Any identifiers (name, alias, postal address, IP address, email, account name, SSN, driver's license number, passport number, or similar)
  - Commercial activity information (products or services purchased, records of personal property, etc.)
  - Biometrics
  - Internet activity (browsing, search history, interaction on a website or application)
  - Geolocation data
  - Audio, electronic, visual, thermal, olfactory or similar information
  - Professional or employment-related information
  - Education information
  - Inferences from any other personal information to create a profile of a consumer
  - Sensitive personal information (e.g., SSN, driver's license #, state ID, or passport #, racial or ethnic origin, precise geolocation, genetic data, contents of consumer communications, health information, biometric information to identify a consumer)

Consumer health data (WA)

Washington “My Health My Data” Act (RCW 19.373(8)(a) and(b)):

- **Consumer health data" means personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status.**

- Examples:

  (i) Individual health conditions, treatment, diseases, or diagnosis;

  (ii) Social, psychological, behavioral, and medical interventions;

  (iii) Health-related surgeries or procedures;

  (iv) Use or purchase of prescribed medication;

  (v) Bodily functions, vital signs, symptoms, or measurements of the information described in this subsection (8)(b);

  (vi) Diagnoses or diagnostic testing, treatment, or medication;

  (vii) Gender-affirming care information;

  (viii) Reproductive or sexual health information;

  (ix) Biometric data;

  (x) Genetic data;

  (xi) Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies;

  (xii) Data that identifies a consumer seeking health care services; or

  (xiii) Any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data described in (b)(i) through (xii) of this subsection that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).

HIPAA or state law

- Many state privacy laws exclude HIPAA covered entities and business associates or protected health information (PHI) from their scope:
  - California Civil Code 1798.145(c) exempts ”[...] protected health information that is collected by a covered entity or business associate [...]"
  - Revised Code of Washington 19.373.100(a) exempts "[…] information that meets the definition of […] protected health information for purposes of [HIPAA]"
- If state law does not provide an exemption, both may apply:
  - HIPAA does not preempt a state law provision if it is related to "privacy of individually identifiable health information" and "more stringent" than the HIPAA rules (see 45 C.F.R. 160.203(b))

AI Laws and Regulations

GARDNER

FDA LAW FIRM

Private-Sector Law (U.S.)

- Biden-era EO repealed/replaced with EO 14179 “Removing Barriers to American Leadership in AI”
- Bi-partisan support led to bill establishing AI Safety Institute at NIST in 2024
- Federal legislation limiting private sector AI use has been proposed – but little momentum to-date
- Utah, California have passed generative AI laws. Colorado an “AI systems” law.

Colorado AI Act (SB 24-205)

- Colorado AI Act regulates AI generally:
  - ""Artificial intelligence system" means any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments."
- "High risk AI systems" or "HRAIS" have higher regulatory burden.
- Attorney general may issue regulations and enforces exclusively
- Feb. 1, 2026

Colorado AI Act (cont.)

- HRAIs are focus of regulation:

  “High-risk artificial intelligence system" means any artificial intelligence system that, when deployed, makes, or is a substantial factor in making, a consequential decision.”

- Exemptions include:
  - HIPAA-regulated covered entities providing non-high risk health care recommendations that a health care provider must act to implement.
  - Technologies approved, authorized, certified, cleared or developed, by federal agency, such as the FDA, or if in compliance with certain federal standards at least ”substantially equivalent” to the Act.

Colorado AI Act (cont.)

- “Developers” of HRAIS must provide “deployers”:
  - Statement of “reasonably foreseeable uses and known harmful or inappropriate uses”
  - Summaries of types of training data used, system purpose, and intended benefits uses
  - Documentation describing how performance was evaluated and mitigation of discrimination, bias and measures to mitigate known/foreseeable risks of discrimination and how the system should be used/not used, and monitored
  - Additional documentation as necessary
  - Facilitate impact assessment by deployer or third party

California – Generative AI Law

- CA Assembly Bill 2013 regulates GenAI:
  - "Artificial intelligence" means an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments. [...]
  - "Generative artificial intelligence" means artificial intelligence that can generate derived synthetic content, such as text, images, video, and audio, that emulates the structure and characteristics of the artificial intelligence's training data.

California Legal Advisory

- California attorney general issued a January 2025 legal advisory on use of AI in health care, emphasizing:
  - Transparency with patients when their information is used to train AI and how providers are using AI to make decisions
  - Not using AI to draft patient notes or other communications that contain erroneous or misleading information
  - Ensuring health care provider decision-making is not supplanted by AI (particularly in payor contexts)
  - Prohibitions on discrimination in health care settings
  - Considering informed consent principles before using AI in treatment settings

Food & Drug Administration (FDA)

- FDA regulates AI/ML enabled medical devices:
  - *Premarket Review:* Devices incorporating AI/ML may require premarket review through 510(k), De Novo, or Premarket Approval (PMA) pathways, depending on their risk classification and intended use.
  - *Software as a Medical Device (SaMD):* FDA has specific regulations for SaMD, including criteria for determining whether software is subject to device regulations.
  - *Real-World Evidence (RWE):* FDA may require RWE to assess the long-term safety and effectiveness of AI/ML-enabled devices.
  - *Algorithmic Bias and Fairness:* Addressing bias in AI algorithms is essential to ensure equitable and effective healthcare.
  - *Transparency and Accountability:* Manufacturers should be transparent about the development, validation, and performance of AI/ML algorithms

Key Considerations

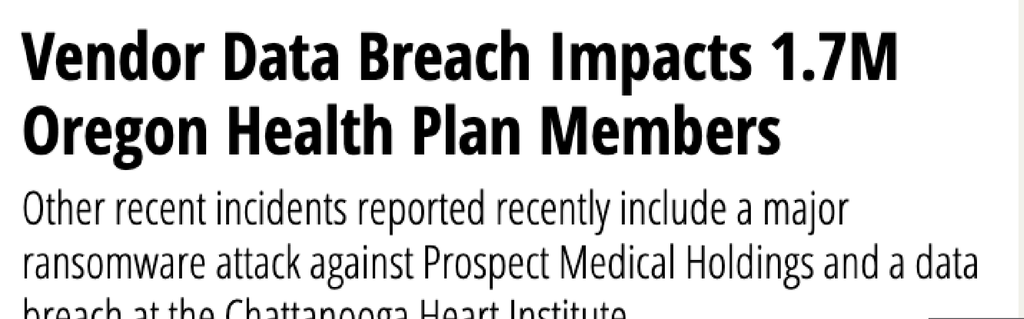
GARDNER

FDA LAW FIRM

Internal use

- Provide appropriate, approved AI tools
  - Personnel will use AI tools, so make sure there are appropriate and secure options
- Implement policies on use and development of AI
  - Company approved AI tools
  - PHI and confidential information restrictions
  - Address privacy and AI risks in development of AI
- Train personnel on AI risks/proper use
- Address AI in privacy and security training

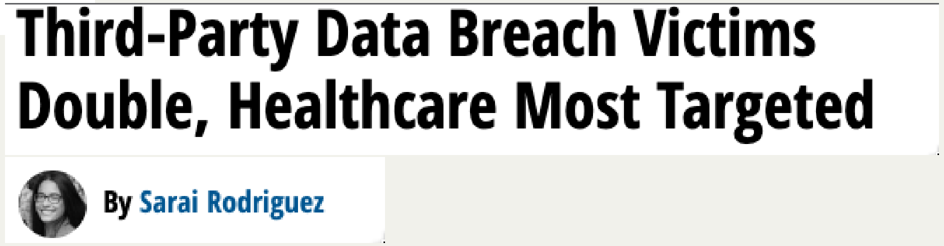
Vendors



Vendor Data Breach Impacts 1.7M Oregon Health Plan Members

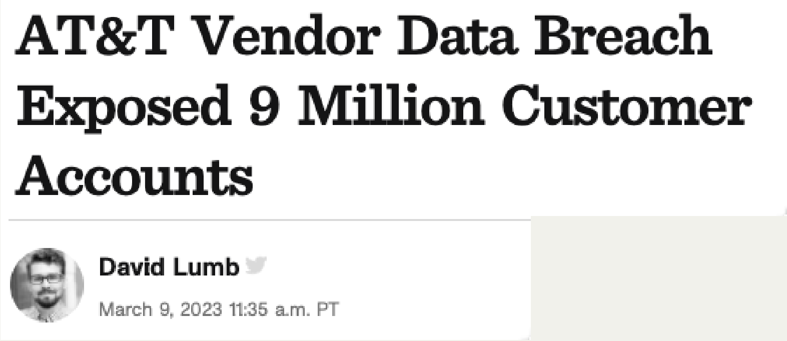
Other recent incidents reported recently include a major ransomware attack against Prospect Medical Holdings and a data breach at the Chattanooga Heart Institute.

By Jill McKeon



Third-Party Data Breach Victims Double, Healthcare Most Targeted

By Sarai Rodriguez



AT&T Vendor Data Breach Exposed 9 Million Customer Accounts

David Lumb

March 9, 2023 11:35 a.m. PT

[1] https://healthitsecurity.com/news/vendor-data-breach-impacts-1.7m-oregon-health-plan-members
[2] https://www.cnet.com/tech/mobile/at-t-vendor-data-breach-exposed-9-million-customer-accounts/
[3] https://healthitsecurity.com/news/third-party-data-breach-victims-double-healthcare-most-targeted

Vendor management

- Implement pre-contractual diligence
  - Security/privacy protections
  - PHI or other confidential information
  - AI use/training
- Use effective, AI-specific contract language
- Business associate agreements
- Ongoing monitoring
  - Revisit (annually, biannually)

Clinical trials

- Get the ICF right
- Avoid misuses of PHI or clinical trial information:
  - Contract language (aim to future proof)
  - Assess vendors, data flow
  - Address offshoring
- Don’t forget the trial master file
  - CVs and other documentation contain personal information

AI system development (general)

- Ensure lawful data use in AI training
  - Assess contractual limitations
  - HIPAA, other privacy laws, consumer expectations
- Ensure AI system itself is compliant
  - Are there ”high risk” health care recommendation?
  - Consider HCP decision-making role
  - FDA cleared/approved?
  - Support customer compliance (PHI use, etc.)
  - Key information about the system to deployers/customers, regulators, and patients (not a black box)

Automated decision-making/agentic AI

- Individual rights (opt-out rights for example) that apply to automated decision-making
- AI agent deployment and legal requirements
  - Access to/sharing PHI (RBAC, minimum necessary)
  - Use and disclosure of PHI (HCO, tx, other?)
  - Human/HCP decision-making
  - Transparency requirements
- Assess for FDA requirements

Questions

GARDNER
FDA LAW FIRM

This presentation is provided as general or educational information only and is not intended to constitute legal or professional advice.